Claims

I Claim:

1. A method of securely comparing a first document in possession of a first party and a second document in possession of a second party, without revealing the contents of the first document to the second party or the contents of the second document to the first party, said method comprising the steps of:

i) said first and second parties each generating its own set of random data;
ii) each party exchanging said set of random data and a shared hash function with the other party;
iii) each party computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data;
iv) each party computing a second value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data;
v) each party sending its first value to the other party and receiving the other party's first value; and
vi) each party comparing said other party's first value to its second value;
vii) each party concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different.

2.. The method according to claim 1 further comprising the steps of:

viii) after computing said first and second values according to steps iii) and iv) above, each said first and second parties sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said

other party that each said party's first and second values have been computed before proceeding; and

ix) after one party has sent its first value to the other party according to step v) above, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time.

3.. The method according to claim 2 further comprising the steps of:

x) after step i) and before step ii), each party examining the other party's set of random data for suitability and aborting the comparison if suitability is not established.

4. The method according to claim 3 wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data.

5. The method according to claim 1 wherein said parties exchange two shared hash functions, a first hash function applied by said first party in step iii) and said second party in step iv) and a second hash function applied by said second party in step iii) and said first party in step iv).

6. The method according to claim 1 wherein said documents are normalized prior to computation of said first and second values to allow the method to ignore inconsequential differences between said documents.

7. The method according to claim 1 wherein said hash function is adapted to act on said documents in a normalized way to allow the method to ignore inconsequential differences between said documents.

8. A computer program product for securely comparing a first document in possession of a first party and a second document in possession of a second party, without revealing the contents of the first document to the second party said computer program product comprising:

a computer usable medium having computer readable program code means embodied in said medium for:
i) generating a set of random data for said first party;
ii) exchanging said set of random data and a shared hash function with the other party;
iii) computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data;

iv) computing a second value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data;

v) sending said first value to the other party and receiving the other party's first value; and
vi) comparing said other party's first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in said other party's possession, followed by said set of random data, followed by the other party's set of random data, to its second value;

vii) concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different.

9. The computer program product of claim 8 wherein said computer usable medium further has computer readable program code means embodied in said medium for:

viii) after computing said first and second values according to iii) and iv) above, sending

confirmation to the other party that the first and second values have been computed, and waiting for confirmation from said other party that said other party's first and second values have been computed before proceeding; and

ix) after sending its first value to the other party according to v) above, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time.

10. The computer program product of claim 9 wherein said computer usable medium further has computer readable program code means embodied in said medium for:

x) after step i) and before step ii) examining the other party's set of random data for suitability and aborting the comparison if suitability is not established.

11. The computer program product of claim 10 wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data.

12. The computer program product of claim 8 wherein said parties exchange two shared hash functions, a first hash function applied by said first party in step iii) and said second party in step iv) and a second hash function applied by said second party in step iii) and said first party in step iv).

13. The computer program product of claim 8 wherein said documents are normalized prior to computation of said first and second values to allow the method to ignore inconsequential differences between said documents.

14. The computer program product of claim 8 wherein said hash function is adapted to act on said documents in a normalized way to allow the method to ignore inconsequential differences between said documents.

15. An article comprising:

a computer readable modulated carrier signal;
means embedded in said signal for securely comparing a first document in possession of a first party and a second document in possession of a second party, without revealing the contents of the first document to the second party by:

i) generating a set of random data for said first party;
ii) exchanging said set of random data and a shared hash function with the other party;
iii) computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data;

iv) computing a second value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data;

v) sending said first value to the other party and receiving the other party's first value; and
vi) comparing said other party's first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in said other party's possession, followed by said set of random data, followed by the other party's set of random data, to its second value;

vii) concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different.

16. The article of claim 15 wherein said signal further has means embodied therein for:

viii) after computing said first and second values according to iii) and iv) above, sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said other party that said party's first and second values have been computed before proceeding; and

ix) after sending its first value to the other party according to v) above, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time.

17. The article of claim 16 wherein said signal further has means embodied therein for

x) after step i) and before step ii) examining the other party's set of random data for suitability and aborting the comparison if suitability is not established.

18. The article of claim 17 wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data.

19. The article of claim 15 wherein said parties exchange two shared hash functions, a first hash function applied by said first party in step iii) and said second party in step iv) and a second hash function applied by said second party in step iii) and said first party in step iv).

20. The article of claim 15 wherein said documents are normalized prior to computation of said first and second values to allow the method to ignore inconsequential differences between said documents.

21. The article of claim 15 wherein said hash function is adapted to act on said documents in a normalized way to allow the method to ignore inconsequential differences between said documents.